Crimes in Connection with Cryptocurrencies

Dr. Dávid Tóth*

Abstract

The aim of the article is analyzing the criminological aspects of cryptocurrency crimes. The use of cryptocurrencies as a payment method is a relatively new social phenomenon, and criminals have found different ways to misuse them. In many countries – like in Hungary – cryptocurrencies are existing in a legal grey area and they are not valued as an official payment method or not even a cash-substitute payment instrument. As a result of this if somebody counterfeits a cryptocurrency that would not be valued as the crime of counterfeiting of cash-substitute payment instruments, and the offender would avoid criminal punishment. It is necessary to give legal answers to this phenomenon to prevent future criminal conducts.

The current study after the overview of the cryptocurrency crimes researches the legal means in the European Union to combat this new form of cybercrime.

Keywords: *cybercrime, cryptocurrency crimes, bitcoin.*

1. Introduction – General remarks about cyber crimes

As the technology evolved and the internet-capable devices spread new opportunities appeared for the offenders. As a result of this nowadays cybercrime is becoming a more and more separate and unique part of the criminal law.[1] The research in connection with cybercrime – as a new trend in criminal justice – aims to give up to date answers to this sui generis phenomenon.

It is not an easy task to give an abstract definition of cybercrime. It also has to be noted that this concept is controversial. In 1991-ben Martin Wasik published a book titled Crime and computer. At this time the internet was not a part of the everyday life of people. The evolution of the cyberspace has changed the criminality entirely. According to Walden cybercrime is part of computer crime. A computer is required to connect to the cyberspace and to commit criminal offence there. In Walden's view internet crime is narrower than computer crime. Hunton had a similar argument when he stated that "digital" and "high-tech" is such a broad area where internet connectivity is not necessarily contrary to the so-called e-crime and cybercrime.[2]

Cybercrime can be classified in many ways. According to one division we can differentiate between crimes committed with computers and the so-called computer-centric crimes. This division is based on that in certain cases the computer only aids in

* Ph.D., Lecturer at the Criminology and Penal Law Department, University of Pécs, Faculty of Law, Hungary. Contact: toth.david@ajk.pte.hu

[1] See: Gál, László István: *The criminal law protection of the stock market is Hungary*. *Economic policy,* Journal of Eastern-European Criminal Law 2015/2, pp. 43-45.

[2] Gillespie, Alisdair A., *Cybercrime.* Routledge. New York, 2015, pp. 1-3.

the crime which already exists in the criminal law. Theft and the distribution of child pornography can be a good example of this. Both crimes existed before the appearance of computers and the internet. On the other cyberspace created the possibility to commit these crimes with easier and more effective methods. Theft can be committed by hacking to an internet bank system or by phishing.[3]

The above-mentioned findings can be applied to the newer virtual phenomenon the cryptocurrencies. There are many ways to misuse these virtual currencies. The aim of the study to give a general overview of crimes related to cryptocurrencies and give possible legal solutions to this problem.

2. The concepts of the cryptocurrencies

According to the Oxford Handbook of Dictionary, the definition of cryptocurrency is the following: *"a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank."* https://www.lexico.com/en/definition/cryptocurrency date of download: 2019. 08. 14.). In Hungary, there is no legal definition for virtual money yet and they exist in a grey area in a legal sense. Under the Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises only established the concept of electronic money which is defined as the following:

- *"electronically, including magnetically, stored monetary value as represented by a claim on the issuer of the electronic money which is issued on receipt of funds for the purpose of making payment transactions as defined in the Act on the Pursuit of the Business of Payment Services, and which is accepted by a natural or legal person, unincorporated business association or private entrepreneur other than the electronic money issuer, excluding the monetary value stored on instruments provided for in Paragraph k) of Subsection (4) or used for the payment transaction defined in Paragraph l) of Subsection (4)".*

Furthermore, cryptocurrencies cannot be valued as cash-substitute payment instruments as well. The Criminal Code of Hungary (Act C of 2012) has an exhaustive listing of cash-substitute payment instruments[4] in the interpretation section (Paragraph 459. 19-20. point) and we cannot find cryptocurrencies there.[5] As a consequence of this, if somebody counterfeits a cryptocurrency that would not be valued as the crime of counterfeiting of cash-substitute payment instruments, the offender would avoid criminal punishment.[6]

---

[3] Gillespie, *cited*, pp. 2-3

[4] See further in: Gál, István László, *A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. [Counterfeiting and stamp forgery]* In: Polt, Péter (editor), Új Btk. kommentár: 7. kötet, Különös rész. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. Budapest. 2013. pp. 193-224; Kőhalmi, László, *A pénzhamisítással kapcsolatos bűncselekmények. A pénz büntetőjogi fogalma. [Crimes related to counterfeiting. The concept of money in criminal law]* In: Balogh, Ágnes – Kőhalmi, László - Büntetőjog II. Különös rész. Dialóg Campus Kiadó, Pécs 2005. pp. 411-417.

[5] Tóth, Dávid, *A bankkártya csalások büntetőjogi szabályozása Németországban. [The regulation of credit card fraud related crimes in Germany]* In: Koncz, István; Szova, Ilona (szerk.), PEME XVI. PhD Konferencia, a 15 éves PEME XVI. PhD - Konferenciájának előadásai. Budapest. 2018. p. 105.

[6] See: Gál, László István: *Economic policy, criminal policy and economic crimes,* Journal of Eastern-European Criminal Law 2019/1, pp. 100-103.

3. Crimes in connection with cryptocurrencies

There were many ways to misuse cryptocurrencies in practice. Without attempting to be exhaustive the following are examples:

- theft,[7]
- fraud,[8]
- Ponzi-scheme,[9]
- Using malicious codes and software against crypto wallets. This is also called as crypto jacking,[10]
- The so-called "Initial Coin Offerings" or ICO-s when fraudsters invite people to spend their money on fake virtual coins.[11]
- In theory, it is possible to commit virtual counterfeiting of money.
- Cryptocurrencies can be used for money laundering.[12]
- They can be used to buy an illegal market like on the darknet.
- They can be used to steal personal information.
- It can be instruments for terrorist financing.[13]
- They can be the means for tax evasion.[14]

As technology evolves newer and newer types of fraud can be committed in connection with cryptocurrencies.

3.1. Theft related to virtual money

According to a Cambridge University study around 3 million people trades actively with cryptocurrencies. The spread and easier access to the online business world resulted that the theft in the cyberspace is increasing. These can be committed against cryptocurrencies as well.[15]

---

[7] Orme, David, *Is biometrics the answer to crypto-currency crime?* In: Biometric Technology Today, 2019/2. p. 8.

[8] Eszteri, Dániel, *Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. [A financial crime committed with a bitcoin and the related legal questions]* In: Infokumminkáció és jog 2017/1. pp. 25-29.

[9] Eszteri, Dániel, A World of Warcraft-tól a Bitcoin-ig. Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. *[From the World of Warcraft to the Bitcoin. The analyses of the status of the individual, the economy, and the money in the virtual communities]:* Doktori értekezés. PTE-ÁJK, Pécs. 2015. pp. 159-161.

[10] Sigler, Karl, *Crypto-jacking; how cybercriminals are exploiting the crypto-currency boom.* In: Computer Fraud & Security, 2018/9, pp. 13–14.

[11] See further in: Zetzsche, Dirk – Ross, Andreas, – Buckley, Ross P. – Arner, Douglas W. – Föhr, Linus, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators* In: Harvard International Law Journal, Vol. 63, 2019/2, pp. 1-39.

[12] Vandezande, Niels, *Virtual currencies under EU anti-money laundering law*. In: Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.011 (date of download 2019. 06. 01.); Gál, István László, *A pénzmosás* [Money laundering]. KJK-Keszöv Jogi és Üzleti Kiadó, Budapest, 2004, pp. 3-15.

[13] Halopeau, Bruno, *Terrorist use of the internet*. In: Akhgar, Babak - Staniforth, Andrew - Bosco, Francesca, (editors) Cyber Crime and cyber terrorism investigator's Handbook. Elsevier. 2014. p. 128.

[14] See further in: Slattery, Thomas, *Taking a bit out of crime: Bitcoin and cross-border tax evasion*. In: Brooklyn Journal of International Law. Vol. 39. 2014/2. pp. 829-873.

[15] Study highlights growing significance of cryptocurrencies. University of Cambridge. 4 May 2017. https://www.cam.acuk/researcli/news/study-highlighrs-growing-significance-of-cryptocurrencics 2019, accessed on 2019. 06. 01.

Researchers also found that the people who invest in cryptocurrencies are not fully aware of the mechanisms of these instruments. They are also not aware of the possible dangers and risks. A study in 2018 conducted by the IW Capital, a Mayfair-based SME investment house found that less than five per cent of the cryptocurrency investors in the United Kingdom could realize the actual profit.[16]

In most part of the world, the regulation of cryptocurrencies is incomplete or not existent. Furthermore, there are no consumer protector rules for cryptocurrency users. So many dollar millions worth of crypto money is lost without recovering them. In 2018 the South Korean crypto exchanger reported that 31.5 million dollars worth of virtual coins were obtained by hackers.[17] These types of attacks are breaching the trust in bitcoin and other similar virtual currencies. A mixture of a public and a private key (which are used for the authentication and encryption of the transaction) resulted that it is difficult to follow such transactions. This is true to the legal and illegal transactions as well.

3.2. Fraud in connection with cryptocurrencies

Dániel Eszteri had wrote a case report[18] which happened in Hungary. The offenders have cheated out a considerable amount worth of bitcoin. Eszteri was an advisor ordered by the court. The two accused persons have visited the victim in winter. Later they met at a parking lot of a store. The perpetrator offered 2.5 million Forints (around 7484 Euros) for 15 units of bitcoin. The victim brought the notebook with him to the parking lot to transfer the bitcoins. He transferred the crypto-money to the address assigned by the offender.

After this, the two perpetrators tried to flee from the scene with their car but eventually, police caught them. At first, time the authorities did not mention in their report that it was a financial crime and even though the victim asked for the seizure of the IT equipment the police failed to do so. Later the indictment contained the crime of fraud which caused a considerable amount of damage. The offenders transferred the bitcoins to several addresses and these were untraceable. The seizure probably would have prevented the loss of the 15-unit bitcoin according to Eszteri.[19] There are many challenges and questions regarding the seizure of cryptocurrencies.[20] The victim made a civil claim in the criminal procedure.

3.3. The ponzi-schemes

Virtual money can be used for ponzi-schemes. A few good examples for this were the OneCoin and the Bitconnect case. The Hungarian National Bank has warned the

---

[16] Memoria, Francisco, *UK Crypto Investors Lack of Knowledge Is "Very Concerning" as Just 5% Make "Financial Gains."* In: CryproGlobe 2018. July. https://www.cryptoglobe.com/latest/2018/07/uk-crypto-investors-lack-of-knowledge-is-very-concerning-as-just-5-make-financial-gains/, accessed on 2019. 09. 01.

[17] Orme, *op. cit.*, pp. 8-10.

[18] Eszteri, *op. cit.,* 2017, pp. 25-29.

[19] Eszteri, *op. cit.,* 2017, p. 28.

[20] See further in: Simon, Béla, *A kriptovaluták és a kapcsolódó rendészeti kihívások. [Cryptocurrencies and challenges in the law enforcement]* In: Mezei, Kitti (editor.) A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs. 2019, pp. 169-186.

retail clients to be cautious with the OneCoin cryptocurrency, because it can be an international disguised ponzi-scheme. The OneCoin had several promises like monthly 5 percent profit or weekly 1 percent profit without any risks. The organization of OneCoin scouted a lot of people on the internet to join the business by offering them a great yield. They paid out the older members with the investment of the newly entered people. In 2010 The Hungarian Financial Supervision made a police report against OneCoin. Not only in Hungary but other foreign countries also had scandals in connection with OneCoin. In 2017, In Italy the Competition authority temporarily banned the company, the One Network Services Ltd, which was responsible for the selling OneCoin. According to the investigation of the authority the company offered unrealistically high in exchange for a 140euro education package. They promised 2800 euro yield within 2 years. (Turzó, 2017)

Another infamous case (which is still going) was the Bitconnect scandal. The Federal Bureau of Investigation (FBI) in it's official website asked people to come forward if they were scammed in connection with Bitconnect. This company also offered high incomes for the investors. If somebody paid in ten thousand dollars the company offered fifty-two thousand dollars pay back within two years.[21]

The so-called Initial Coin Offerings (ICO-s) are similar to Ponzi-schemes. The perpetrators create a fake or non-existent virtual money and after a major marketing campaign, they persuade people to buy their coins. They promise high income within a short period time. Many people can be manipulated to buy their fake coins with the so-called fear of missing out (FOMO) psychological tactic. This method is called a quick fund-raising. The investors usually lack the knowledge of the topic and they only look at the promised incomes. A good example for the ICO scam can be the Prodeum cryptocurrency. The Prodeum used the blockchain of another cryptocurrency: Ethereum. They managed to elicit around three thousand dollars with ICO-s. The company in connection with Bitflur and the Magnalis cryptocurrency also used a similar technique. Under the report of the Enrst & Young in 2017 2017 around 400 million damage was caused by the offenders with the ICO-s.[22]

3.4. The crypto jacking

As Saad, Khormali and Mohaisen defined in their paper *"crypto jacking is the use of system resources of a target device to compute hashes and make profit out of mining without the consent of the target device's owner."*[23] The new phenomenon of crypto jacking has two forms. On one hand there is the browser based crypto jacking.[24] Usually, this malicious activity is executed through scripts that are running within a website. The mechanism of this can be summarized in the following example. The

---

[21] https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-in-bitconnect-investigation 2019, accessed on 2019.07.15.

[22] Crypto-currencies hit by hacking attacks, theft and fraud. (2018). *Network Security, 2018(2),* pp. 1–2. http://doi.org/https://doi.org/10.1016/S1353-4858(18)30011-4.

[23] Saad, Muhammad, - Khormali, Aminollah - Mohaisen, Aziz, End-to-end analysis of in-browser cryptojacking. In: arXiv:1809.02152v1 [cs.CR] 6 Sep 2018, https://arxiv.org/pdf/1809.02152.pdf, accessed on 2019.07.15.

[24] Eskandari, Shayan – Leoutsarakos, Andreas – Mursch, Troy – Clark, Jeremy: *A First Look at Browser-Based Cryptojacking*. In: arXiv:1803.02887v1 [cs.CR] 7 Mar 2018, pp. 58–59. https://arxiv.org/pdf/1803.02887.pdf, accessed on 2019.07.01.

offender attacks a company network. The attacker recognizes a vulnerable website and hides malicious code on the internet site unbeknown to the user. When an employee, the corporate user logs in to the site to check the news, thanks to the malicious crypto jacking code this user is now the processing power for the attacker. The user's computer will become the mine for digital currency. As long as the web browser is open the offender benefits. Harnessing the users machine the attacker performs a computation needed to update blockchain and release new cryptocurrency. The mined currency is deposited into the electronic wallet of the offender while the cost on mining is worn by the user. Attackers decided to use this new method for a number of reasons. On the other hand, we can talk about the file based crypto jacking.

These attacks work like any other malwares. Usually they are self-propagating. They get in and spread thru the network and they cause huge cleanup cost. There are many reasons why criminals use this method. Firstly, they want to get money quickly, efficiently and easily. It only requires a simple script and browser based crypto jacking does not require the same level of skill from traditional threats. Some organizations are slow to recognize the dangers of crypto jacking. Crypto jacking is a stealthy method. Users usually only notice that their computer is becoming slower, and the electricity bill is rising. The increasing cryptocurrency value is also an important factor.[25]

Guillermo Suarez-Tangil from the King's College London University and Sergio Pastrana from the Charles III University of Madrid analyzed 4.4 million crypto jacking malware code. The malicious codes were used between 2007 and 2018 by criminals. According to their estimate crypto jacking produced 57 million dollars profit for the offender around the world. One of the largest organized crime[26] reached alone 18 millions dollar income.[27]

It is not easy to detect these crypto jacking malwares but there are browser extensions that are able to effectively prevent most crypto jacking attacks (like minerblocker add-on in the Mozilla Firefox browser).

3.5. Virtual money counterfeiting as a theoretical possibility

Virtual money counterfeiting is basically when a person transfers a virtual money twice (like one Bitcoin twice). In a technical sense this is impossible at the time of the writing. We can show this on the example of bitcoin. Bitcoin is not a computer file which can be copied two or more times. Bitcoin only exists in a ledger as a value. The ledger registers all of the bitcoin transactions in the History.

Every person who uses a bitcoin owns a copy of a ledger. If somebody wants to spend two bitcoins when in reality he has only one he has to modify all the ledgers in the world. Even if he can hack to some computers it is impossible to do this globally. The unhacked computers with the true copy of ledger will signal that the counterfeiter only actually has one bitcoin, most of the ledgers have to verify the bitcoin transaction to become completed. Due to fact that.[28]

---

[25] Sigler, *cited,* pp. 13-14.

[26] See: Tóth, Dávid – Gál, István László – Kőhalmi, László, *Organized crime in Hungary*, Journal of Eastern-European Criminal Law 2015/1, pp. 22-23.

[27] Stokel-Walker, Chris, *Are hackers making money with your PC?* In: New Scientist, 2019/1, p. 6.

[28] Eszteri, *cited,* 2015, p. 129.

4. Combatting cryptocurrency crimes in the European Union with legal means

4.1. The new Directive Proposal of the European Commission

The European Commission proposed a new Directive on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA for the European Parliament and the Council. The European Union adopted the Directive in 17th of April 2019. This Directive aimed to modernize the previously existing EU legislation. The new legal source sets minimum rules in connection with the punishability of the non-cash payment instrument frauds in a more effective way. According to the European Commission the earlier regulation was not reflecting the reality and does not deal with actual problems due to the revolution of information technology (like the appearance of cryptocurrencies and mobile payments). The non-cash payment instrument frauds contribute to other crime forms like:

- organized crime groups;
- terrorism;
- drug trafficking;
- human trafficking.

The Commission in its Directive proposal set three goals:

- to guarantee clear, established and technological neutrality in the regulation.
- Operational barriers that limit investigation and prosecution should be eliminated.
- Lastly the EU should improve prevention.

4.2. The opinion of the European Economic and Social Committee

The European Economic and Social Committee (EESC) in the January of 2018 released an opinion about the new Directive proposal [COM(2017) 489 final – 2017/0226 (COD)]. The EESC had constructive findings. On one hand the EESC was positive about that the Commission aims to modernize the regulation in this area, because the fight against computer crimes should be a priority in the European Union while the electronic payments are becoming more widespread. The EESC agreed that the previous regulation was outdated and new rules are necessary to protect the information society. Overall, they acknowledge the aims of the Directive proposal.

I would highlight the following parts of the opinion:

- The Directive in the jurisdiction of investigation part (Article 11) must be clarified whether the fundamental principle is the location of the person or of the information system or computer used in order to avoid any conflict of jurisdiction. They propose to amend with a subpoint on settling conflicts of jurisdiction using one of the two methods mentions.

- They think that there may be some bewilderment regarding the subject of the Directive so they propose amending the title and replacing the phrase non-cash payment with electronic and digital means of payment.

4.3. The history of the Directive proposal

After the release opinion the European Parliament asked the Civil Liberties, Justice and Home Affairs Committee (LIBE) and Sylvia-Yvonne Kaufmann rapporteur,

to give another opinion on the Directive proposal.[29] The Europol gave a report in the September of 2018 about the organized crime activities on the internet which reviewed the fraud related to internet payment and the skimming of ATM-s and POS terminals. The telecommunication misuse is a big challenge for the law enforcement.

At the end of 2018. the European Parliament and the Council have established a formal agreement regarding the Directive Proposal. The two parties agreed in the following point:

- it is necessary to harmonize the crimes online, such as hacking and phishing.
- It is important to give a minimal legal framework for sanctions. The Directive should contain at least one to five years imprisonment commensurate with the gravity of the crime.
- There should be more effective legal and non-legal means to conduct investigations.
- The scope of the law should protect the virtual money transactions as well.
- The prevention and the protection of victims should be enhanced.

The Council informed the head of the LIBE that they accept the European Parliament's standpoint and approve the regulation in this for.

The plenary session was held in March 2019.[30] The Directive proposal was adopted on 17th of April 2019 in an ordinary legislative procedure.

4.4. The rules of the new Directive

The Directive has the title of "combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA." In the first article they drafted that the main goal is prevention and the of assistance to and support for victims. The accepted Directive contains the following crimes which are punishable:

- Fraudulent use of non-cash payment instruments.
- Offences related to the fraudulent use of corporeal non-cash payment instruments.
- Offences related to the fraudulent use of non-corporeal non-cash payment instruments.
- Fraud related to information systems.
- Preparation, Incitement, aiding and abetting and attempt of these offences.

Fraudulent use of non-cash payment instruments means when a person uses a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument. Under the Directive the fraudulent use of a counterfeit or falsified non-cash payment instrument is also punishable in this category. (Directive Article 3)

The second crime group consist the following conducts:

- the theft or other unlawful appropriation of a corporeal non-cash payment instruments.
- Counterfeiting or falsification of a corporeal non-cash payment instrument.
- The possession of a stolen or otherwise unlawfully appropriated, or of a counterfeit or falsified corporeal non-cash payment instrument for misuse.

---

29 http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file- combating-fraud-counterfeiting-of-non-cash-means-of-payments 2019, accessed on 2019. 09. 01.

30 http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-counterfeiting-of-non-cash-means-of-payments, accessed on 2019. 09. 01.

- Lastly the procurement for oneself or another of a stolen, counterfeit or falsified corporeal non-cash payment instrument for fraudulent use. Typically, the receipt, appropriation, purchase, transfer, import, export, sale, transport or distribution is punishable. (Article 4.)

It is novelty in the Directive that the crimes related to immaterial non-cash payments are regulated separately. The unlawful obtainment of these are punishable and Article 5 uses a referential disposition to the Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013/40/EU). If a person unlawfully obtains another person immaterial non-cash payment instrument with

- illegal access to information systems
- illegal system interference
- illegal data interference or
- illegal data interception should be punishable by the Member States.

The third crime besides the above mentioned consists of the following punishable conducts as well:

- the fraudulent counterfeiting or falsification of a non-corporeal non-cash payment instrument;
- the holding of an unlawfully obtained, counterfeit or falsified non-corporeal non-cash payment instrument for fraudulent use, at least if the unlawful origin is known at the time of the holding of the instrument;
- the procurement for oneself or another, including the sale, transfer or distribution, or the making available, of an unlawfully obtained, counterfeit or falsified non-corporeal non-cash payment instrument for fraudulent use. (Article 5.)

One of most significant novelty contrary to the previous regulation that the Directive contains the fraud related to information system. In this section the transfer of virtual currency (or money) with causing unlawful loss of property for another person to make an unlawful gain is punishable when committed intentionally by

- without right, hindering or interfering with the functioning of an information system;
- without right, introducing, altering, deleting, transmitting or suppressing computer data. (Article 6).

The Directive under the "tools used for committing offence" (Article 7) regulates preparatory conducts. According to this part the Member States should take the necessary measures to ensure that producing, procurement for oneself or another, including the import, export, sale, transport or distribution, or making available a device or an instrument, computer data or any other means primarily designed or specifically adapted for the purpose of committing any of the above mentioned crimes, at least when committed with the intention that these means be used, is punishable as a criminal offence.

The Directive differentiates between non-cash payment instrument and virtual currency. Any non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange are considers as non-cash payment instruments. Contrary to this any digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily

attached to a legally established currency and does not possess a legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically shall be considered as a virtual currency. For example, traveller's cheques, promissory are valued as non-cash payment instruments, bitcoin and Ethereum as virtual currencies. (Article 2)

There are different sanctions for people and legal persons. It is a common requirement against the punishments that they shall be preventive, proportional, and effective. The Directive only sets a minimum guideline not the concrete sanction.

- The theft, counterfeiting and falsification of material non-cash payment instruments the maximum penalty shall be at least 2 years of imprisonment. This sanction shall also be applied in the case of the unlawful obtainment, counterfeiting and falsification of immaterial non-cash payment instruments and every preparation type of conduct.
- The possession of unlawfully procured, counterfeited or falsified non-cash payment instrument with fraudulent intention shall be punished with a maximum of years imprisonment. This rule is also applied to the same conducts in connection with immaterial non-cash payment instruments.
- In regard to information system fraud maximum sanction shall be at least three years of imprisonment.
- The Directive deals with aggravated cases, when a person commits this crime in a criminal association the maximum punishment shall be at least five years of imprisonment (Article 9).

Legal persons[31] have special liability[32] rules.[33] They can be held responsible for the above-mentioned offences if the crimes are committed for their benefit by any person acting either individually or as a part of an organ of the legal person, and having a leading position within the legal (like a power of representation)

Furthermore, Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of any of the above-mentioned offences for the benefit of the legal person by a person under its authority.

The Directive also stipulates that the liability of legal persons shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences.

There is one compulsory sanction according to the Directive: fine, even if it is called non-criminal law fine. Facultative sanctions are the following:

- exclusion from entitlement to public benefits or aid;
- temporary exclusion from access to public funding, including tender procedures, grants and concessions;
- temporary or permanent disqualification from the practice of commercial activities;

---

[31] Kőhalmi, László, *A jogi személy büntetőjogi felelőssége* [Criminal liability of the legal person]. Collega 2000/2, pp. 18-21.

[32] Kőhalmi, László, *A jogi személyekkel szemben alkalmazható büntetőjogi* intézkedések [Applicable criminal measures against legal persons]. JURA 2006/1, pp. 53-57.

[33] See: Kőhalmi, László, *Some issues of criminal liability by reason of economic decisions*, Journal of Eastern-European Criminal Law 2019/1, pp. 44-47.

- judicial winding-up;
- placing under judicial supervision;
- temporary or permanent closure of establishments which have been used for committing the offence.

The Directive also establishes rules for jurisdiction in order to speed up the criminal proceedings. Every Member State shall take the necessary measures to establish its jurisdiction over the above-mentioned offences where one or more of the following apply:

- the offence is committed in whole or in part on its territory;
- the offender is one of its nationals.

An offence shall be considered to have been committed in whole or in part on the territory of a European Union Member State where the offender commits the offence when physically present on that territory and irrespective of whether the offence is committed using an information system on that territory. Lastly there is a notification obligation for a Member State to the Commission when it decides to establish jurisdiction over an offence referred to in the offences committed outside its territory, including where:

- the offender has his or her habitual residence in its territory;
- the offence is committed for the benefit of a legal person established in its territory;
- the offence is committed against one of its nationals or a person who is a habitual resident in its territory. (Article 12)

There also obligation for the Member states to exchange information quickly, and effectively to ensure the effective cooperation in criminal matters (Article 13-15)

Article 16 should be also highlighted because the victim support was missing in the previous regulation. The EU Member States shall ensure that natural and legal persons who have suffered harm as a result of any of the offences being committed by misusing personal data are:

- offered specific information and advice on how to protect themselves against the negative consequences of the offences, such as reputational damage; and
- provided with a list of dedicated institutions that deal with different aspects of identity-related crime and victim support.

Also, a positive solution that the Directive encourages Member States to set up a single national online information tools to facilitate access to assistance and support for natural or legal persons who have suffered harm as a result of the crimes being committed by misusing personal data.

The Directive also deals with legal persons as victims. They shall be offered the following information without undue delay after their first contact with a competent authority:

- the procedures for making complaints with regard to the offence and the victim's role in such procedures;
- the right to receive information about the case in accordance with national law;
- the available procedures for making complaints if the competent authority does not respect the victim's rights in the course of criminal proceedings;
- the contact details for communications about their case. (Article 16).

Prevention is one of the main goals of the Directive and it is regulated in Article 17 in detail.

According to this Member States shall take appropriate action, including through the internet, such as information and awareness-raising campaigns and research and education programmes, aimed to reduce overall fraud, raise awareness and reduce the risk of becoming a victim of fraud. Where appropriate, Member States shall act in cooperation with stakeholders.

Article 18 deals with the monitoring of the implementation of the Directive by Member States. By 31 August 2019, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Directive. The monitoring programme shall set out the means by which and the intervals at which the necessary data and other evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting, sharing and analysing the data and other evidence. The Member States should bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 May 2021 and report this to the Commission (Article 18-20).

5. Summary and proposals

According to my view, the new Directive is a positive legal mean combatting the challenges in connection with fraud[34] related to electronic payment and virtual currencies. This will modernize the regulation in the Member States and create a legal harmonization which can suppress also the so-called forum shopping phenomenon when the offenders try to commit crimes in the state where the prescribed sanction is the lowest.

The Directive is also progressive that it deals with the phenomenon of virtual currencies because these transactions shall also be protected by criminal law measures.

References

1. Eskandari, Shayan – Leoutsarakos, Andreas – Mursch, Troy – Clark, Jeremy: *A First Look at Browser-Based Cryptojacking*. In: arXiv:1803.02887v1 [cs.CR] 7 Mar 2018. pp. 58–66. https://arxiv.org/pdf/1803.02887.pdf, accessed on 2019. 07. 01.

2. Eszteri, Dániel, A World of Warcraft-tól a Bitcoin-ig. Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. *[From the World of Warcraft to the Bitcoin. The analyses of the status of the individual, the economy, and the money in the virtual communities]:* Doktori értekezés. PTE-ÁJK, Pécs. 2015.

3. Eszteri, Dániel, *Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. [A financial crime committed with a bitcoin and the related legal questions]* In: Infokumminkáció és jog 2017/1. pp. 25-31.

4. Gál, István László, *A pénzmosás* [Money laundering]. KJK-Keszöv Jogi és Üzleti Kiadó, Budapest, 2004.

5. Gál, István László, *A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. [Counterfeiting and stamp forgery]* In: Polt, Péter (editor), Új Btk. kommentár: 7. kötet, Különös rész. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. Budapest. 2013. pp. 193-224.

[34] See: Kőhalmi, László, *The never-ending fight: economic and political corruption in Hungary*, Danube: Law and Economics Review 2013/4, pp. 67-71.

6. Gál, László István: *The criminal law protection of the stock market is Hungary*.Journal of Eastern-European Criminal Law 2015.2. pp. 43-49.

7. Gál, László István: *Economic policy, criminal policy and economic crimes,* Journal of Eastern-European Criminal Law 2019/1, pp. 100-109.

8. Gillespie, Alisdair A., *Cybercrime.* Routledge. New York, 2015.

9. Halopeau, Bruno, Terrorist use of the internet. In: Akhgar, Babak – Staniforth, Andrew – Bosco, Francesca, (editors) Cyber Crime and cyber terrorism investigator's Handbook. Elsevier. 2014. pp. 123-132.

10. http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-counterfeiting-of-non-cash-means-of-payments 2019, accessed on 2019. 09. 01.

11. http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-counterfeiting-of-non-cash-means-of-payments 2019, accessed on 2019. 09. 01.

12. https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-in-bitconnect-investigation 2019, accessed on 2019. 07. 15.

13. Kőhalmi, László, *A jogi személy büntetőjogi felelőssége* [Criminal liability of the legal person]. Collega 2000/2. 18-23.

14. Kőhalmi, László, *A pénzhamisítással kapcsolatos bűncselekmények. A pénz büntetőjogi fogalma. [Crimes related to counterfeiting. The concept of money in criminal law]* In: Balogh, Ágnes – Kőhalmi, László – Büntetőjog II. Különös rész. Dialóg Campus Kiadó, Pécs 2005. pp. 411-417.

15. Kőhalmi, László, A jogi személyekkel szemben alkalmazható büntetőjogi intézkedések [Applicable criminal measures against legal persons]. JURA 2006/1, pp. 52-62.

16. Kőhalmi, László, *The never-ending fight: economic and political corruption in Hungary*, Danube: Law and Economics Review 2013/4. pp. 67-82.

17. Kőhalmi, László, *Some issues of criminal liability by reason of economic decisions*, Journal of Eastern-European Criminal Law 2019/1. pp. 44-52.

18. Memoria, Francisco, *UK Crypto Investors Lack of Knowledge Is "Very Concerning" as Just 5% Make "Financial Gains."* In: CryproGlobe 2018. July. https://www.cryptoglobe.com/latest/2018/07/uk-crypto-investors-lack-of-knowledge-is-very-concerning-as-just-5-make-financial-gains/, accessed on 2019. 09. 01.

19. Orme, David, *Is biometrics the answer to crypto-currency crime?* In: Biometric Technology Today, 2019/2, pp. 8-10.

20. Saad, Muhammad, – Khormali, Aminollah – Mohaisen, Aziz, End-to-end analysis of in-browser cryptojacking. In: arXiv:1809.02152v1 [cs.CR] 6 Sep 2018. https://arxiv.org/pdf/1809.02152.pdf, accessed on 2019. 07. 15.

21. Sigler, Karl, *Crypto-jacking; how cybercriminals are exploiting the crypto-currency boom.* In: Computer Fraud & Security, 2018/9, pp. 12-14.

22. Simon, Béla, *A kriptovaluták és a kapcsolódó rendészeti kihívások. [Cryptocurrencies and challenges in the law enforcement]* In: Mezei, Kitti (editor.) A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs. 2019. pp. 169-186.

23. Slattery, Thomas, *Taking a bit out of crime: Bitcoin and cross-border tax evasion*. In: Brooklyn Journal of International Law. Vol. 39. 2014/2. pp. 829-873.

24. Stokel-Walker, Chris, *Are hackers making money with your PC?* In: New Scientist, 2019/1. p. 6.

25. Study highlights growing significance of cryptocurrencies. University of Cambridge. 4 May 2017. https://www.cam.acuk/researcli/news/study-highlighrs-growing-significance-of-cryptocurrencics 2019, accessed on 2019. 06. 01.

26. Tóth, Dávid – Gál, István László – Kőhalmi, László, *Organized crime in Hungary*, Journal of Eastern-European Criminal Law 2015/1, pp. 22-27.

27. Tóth, Dávid, *A bankkártya csalások büntetőjogi szabályozása Németországban. [The regulation of credit card fraud related crimes in Germany]* In: Koncz, István; Szova, Ilona (szerk.), PEME XVI. PhD Konferencia, a 15 éves PEME XVI. PhD – Konferenciájának előadásai. Budapest. 2018, pp. 100-112.

28. Vandezande, Niels, *Virtual currencies under EU anti-money laundering law*. In: Computer Law & Security Review: The International Journal of Technology Law and Practice. 2017, pp. 343-353.

29. Zetzsche, Dirk – Ross, Andreas, – Buckley, Ross P. – Arner, Douglas W. – Föhr, Linus, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators* In: Harvard International Law Journal, Vol. 63, 2019/2, pp. 1-39.